GLOSSARY

Access: The ability to make use of any information system (IS) resource. (Defined in NIST SP 800-32, Section 9).

Access Control: Enables authorized use of a resource while preventing unauthorized use or use in an unauthorized manner. (Defined in NIST SP 800-27, Appendix B).

Accreditation: The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operation (including mission, function, image, or reputation), agency assets, or individuals based on the implementation of an agreed-upon set of security controls. (Defined in NIST SP 800-37, Appendix B).

Administrative Controls: Safeguards to ensure proper management and control of information and information systems. These safeguards include policy, the completion of Privacy Impact Assessments (PIAs), certification and accreditation programs, etc. (Defined in NIST SP 800-12).

Agency: Any executive department, military department, government corporation, or other establishment in the Executive Branch of Government (including the Executive Office of the President) or any independent regulatory agency.

Alien: A person who comes from a foreign country who is not a U.S. citizen nor lawfully admitted for permanent residence in the U.S.

Awareness, Training, and Education: Includes (1) awareness programs that set the stage for training by changing organizational attitudes towards realization of the importance of security and the adverse consequences of its failure; (2) teaching people the skill that shall enable them to perform their jobs more effectively; and (3) education is more in-depth than training, and is targeted for security professionals and those whose jobs require expertise in IT security. (Defined in NIST SP 800-26, Appendix C).

Certificates of Confidentiality: Section 301(d) of the Public Health Service Act, 42 U.S.C. 241(d), provides that the Secretary of HHS may authorize persons engaged in biomedical, behavioral, clinical, or other research (including research on mental health or the use of drugs or alcohol) to protect the privacy of research subjects by withholding from persons not connected with the research the names or other identifying characteristics of such individuals including from compelled legal disclosure processes such as subpoenas for documents or testimony or court orders. Confidentiality certificates do not protect information from voluntary disclosure or when release is requested by the subject individual. Certificates of Confidentiality are issued by the National Institutes of Health.

Certification: A comprehensive assessment of the management, operational and technical security controls in an information system made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operated as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (Defined in NIST SP 800-37, Appendix B).

Children's Online Privacy Protection Act (COPPA) of 1998: Applies to private sector websites that collect personal information online from children under the age of 13. OMB Memorandum M-00-13, *Privacy Policies and Data Collection on Federal Web Sites* extended the provisions of *COPPA* to federal websites. *COPPA* identifies the content that a website operator must include in a privacy policy, outlines when and how to seek verifiable consent from a parent, and specifies the responsibilities an operator has for protecting children's privacy and safety online. (Defined in Secure One HHS Information Security Program Privacy Impact Assessment (PIA) Guide).

Clinger-Cohen Act of 1996: Includes both the *Information Technology Management Reform Act* and the *Federal Acquisition Reform Act* and is intended to improve the productivity, efficiency, and effectiveness of federal programs through the improved acquisition, use, and disposal of IT resources. Among other effects, it makes agencies responsible for IT resource acquisition and management, under the guidance of the Chief Information Officer (CIO), and emphasizes that value must be maximized and risk must be minimized in capital planning and budget processes. In effect, the *Clinger-Cohen Act* places the burden of incorporating privacy controls into IT investments at the agency and CIO levels. (Defined in Secure One HHS Information Security Program Privacy Impact Assessment (PIA) Guide).

Computer Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practice. (Defined in NIST SP 800-61).

Computer Matching and Privacy Protection Act of 1988: Added several new provisions to the Privacy Act of 1974. "Computer matching" occurs when federal and/or state agencies share information in identifiable form (IIF). Agencies use computer matching to conduct many government functions, including establishing or verifying eligibility for federal benefit programs, or identifying payments/debts owed to government agencies. The Act requires agencies engaged in computer matching activities to:

- Provide notice to individuals if their IIF is being computer matched:
- Allow individuals the opportunity to refute adverse information before having a benefit denied or terminated; and
- Establish data integrity boards to oversee computer-matching activities.

(Defined in Secure One HHS Information Security Program Privacy Impact Assessment (PIA) Guide).

Computer Security Act of 1987: Provides a computer standards program within the National Institute of Standards and Technology to provide for Government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems, and for other purposes.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (Defined in 44 U.S.C., Section 3542).

Cookie: Information that a website puts on an individual's computer so that it can remember something about the user at a later time. (See also: Persistent Cookie and Session Cookie).

Data: Programs, files or other information stored in, or processed by, a computer system.

Data Integrity: Assurance of reliability and accuracy of information. The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. (Defined in NIST SP 800-27, Appendix B).

Data Owner: The authority, individual, or organization that has original responsibility for the data by statute, executive order, or directive. (Defined in Secure One HHS Information Security Program Certification and Accreditation Guide).

Database: A set of related files that is created and managed by a database management system.

E-Government Act of 2002: Title II of the E-Government Act of 2002 requires federal agencies to conduct PIAs before developing or procuring IT systems that collect, maintain, or disseminate IIF. Once completed, the agency's Chief Information Officer (CIO), or an equivalent official, must review the Privacy Impact Assessments (PIAs). Additional requirements include making PIAs publicly accessible and posting a machine-readable privacy notice on publicly facing websites. (Defined in HHS Information Security Program Privacy Impact Assessment (PIA) Guide).

Excepted: Records compiled in reasonable anticipation of a civil action or proceeding for which access under the Privacy Act is not granted. (Defined in U.S.C. Section 552a(d)(5) of the Privacy Act).

Exempted: Systems of records for which general and specific exemptions can be claimed to prevent release under some requirements of the Privacy Act. (Defined in U.S.C. Section 552a(j)(k) of the Privacy Act).

Federal Information Security Management Act (FISMA) of 2002 (Title III of E-Gov): Provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. This act defines terms such as information security and information technology and the responsibilities of federal agencies regarding information security. This act also outlines the requirements for annual independent evaluations, which evaluate the effectiveness of an agency's security program and practice. (Defined in HHS Information Security Program Privacy Policy).

Freedom of Information Act (FOIA) of 1966: Requires all agencies of the executive branch to disclose federal agency records or information upon receiving a written request from any individual, except for those records (or portions of them) that are protected from disclosure by certain exemptions and exclusions. (Defined in HHS Information Security Program Privacy Impact Assessment (PIA) Guide). FOIA protects the rights of the public to access Government information and makes provisions for individuals to obtain information on the operation of federal agencies.

General Support System: An interconnected set of information resources under the same direct management control, which shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, and people. A GSS can be, for example, a local area network (LAN), including smart terminals that support a branch office, an agency-wide backbone, a communications network, a departmental data processing center and its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO). (Defined in Office of Management and Budget (OMB) Circular A-130, (A)(2)(c).)

Health Insurance Portability and Accountability Act (HIPAA) of 1996: Affects the health insurance industry and contains provisions under the heading of "Administrative Simplification" that govern how government and private senior health care institutions handle protected health information (PHI), a subset of "individually identifiable health information." Pursuant with these provisions, regulations published in 2000 established standards for providing notice on how to use and disclose health information collected from users under a covered entity's services. These regulations also grant certain rights to individuals, including the right to see one's health records and to request corrections or other amendments to those records. These regulations apply to both written and oral PHI. (Defined in HHS Information Security Program Privacy Impact Assessment (PIA) Guide).

Homeland Security Presidential Directive 12 (HSPD-12): Presidential directive requiring the definition of a set of common, acceptable, and achievable standards for Personal Identity Verification (PIV) of Federal employees and contractors.

Incident: A violation of imminent threat of violation of computer security policies, acceptable use policies, or standard computer security. (Defined in NIST SP 800-61, Appendix D).

Individual: An individual, for the purposes of the Privacy Act, is an American citizen or an alien lawfully admitted for permanent residence.

Information: Any communication or representation of knowledge such as facts, data, or opinions in any medium or form; including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. (Defined in OMB Circular A-130, 6(a)).

Information in Identifiable Form (IIF): Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. (Defined in the E-Government Act of 2002, Public Law 107-347, Title II and III).

Information in an information system or online collection:

- That directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc); or
- By which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic identifier, and other descriptors). (Defined in OMB Memorandum M-03-22, *Guidance for Implementing Privacy Provisions of the E-Government Act of 2002*).

  Note: The acronyms IIF and PII are often used interchangeably.

Information Technology: Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. Equipment is considered used by an executive agency if used directly or is used by a contractor under a contract with the executive agency, which: (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (Defined in 40 U.S.C., Section 1401).

Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. (Defined in 44 U.S.C., Section 3542).

Maintain: To maintain, collect, use or disseminate.

Major Application: An application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunication components. MAs can be either a major software application or a combination of hardware and software in which the only purpose of the system is to support a specific mission-related function. (Defined in NIST Special Publication 800-18). Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as a "Major Application." Adequate security for other applications should be provided by security of the systems in which they operate. (Defined in OMB Circular A-130, (A)(2)(d).)

Major Change: Any change that is made to the system environment or operation of the system. According to OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, PIAs should be conducted following any major changes, including, but not limited to:

- Conversions: A conversion from paper-based methods to electronic systems;
- Anonymous to Non-Anonymous: When the system's function, as applied to an existing information collection, changes anonymous information into IIF;
- Significant System Management Changes: In the case that new uses of an existing IT system, including application of new technologies, significantly change the process of managing IIF in the system;
- Significant Merging: When agencies adopt or alter business processes so that government databases holding IIF are merged, centralized, matched with other databases, or otherwise significantly manipulated;
- New Public Access: When user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system, which can be accessed by the public;
- Commercial Sources: When IIF is obtained from commercial or public sources and is systematically integrated into the existing information systems databases;
- New Interagency Uses: When agencies work together on shared functions involving significant new uses or exchanges of IIF;
- Internal Flow or Collection: When alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional IIF; and
- Alteration in Character of Data: When new IIF added to a collection raises the risk to personal privacy, such as the addition of health or privacy information. (Defined in Secure One HHS Information Security Program Privacy Impact Assessment (PIA) Guide).

Need to Know: The necessity for access to or knowledge of or possession of specific information required to carry out official duties.

NIH Senior Official for Privacy (SOP): A title extended by the Department to NIH to effectively meet the reporting requirements outlined in OMB Memorandum M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. (Defined in Secure One HHS Information Security Program Privacy Impact Assessment (PIA) Guide).

Non-Exempt System: A Privacy Act system of record for which no exemption is claimed for the system. It typically means the record in the system is releasable to the subject of the file. Naturally, there are some exceptions to the rule.

Nonresident Alien: An individual who is not a citizen or national of the United States and who is in this country on a visa or temporary basis and does not have the right to remain indefinitely.

Paperwork Reduction Act (PRA) of 1995: Focuses on increasing the efficiency of the federal government's information collection practices. The *PRA* specifies that Chief Information Officers (CIOs) shall improve protection for the privacy and security of information under their agency's control. The *PRA* also created the Office of Information and Regulatory Affairs (OIRA) within OMB to provide central oversight of information management activities across the federal government. Furthermore, the *PRA* requires agencies to receive an OMB information collection approval number (also known as an "OMB control number") for an information system, prior to using that system to collect information from any person. (Defined in Secure One HHS Information Security Program Privacy Impact Assessment (PIA) Guide).

Persistent Cookie: A cookie that is stored on the user's hard drive and remains there until the user deletes it or it expires.

Personal Identifier: Any piece of information specific to a person such as name, date of birth, medical records, social security number, photographic identifiers etc., used on an IT system to identify a person.

Personally Identifiable Information (PII): Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. (Defined in OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*). Note: The acronyms PII and IIF are often used interchangeably.

Physical Security Controls: Measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. These safeguards might include protections against fire, structural collapse, plumbing leaks, physical access controls, and controls against the intercept of data. (Defined in NIST SP 800-12).

Plan of Action and Milestones (POA&M): A tool that identifies tasks that need to be accomplished. POA&MS identify resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. (Defined in OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*).

Privacy: Freedom from unauthorized and unwarranted intrusion. Under the Privacy Act, it is a set of fair information practices to ensure that an individual's personal information is accurate, secure, and current, and that individuals know about the uses of their data.

The Privacy Act of 1974, as amended: Protects the privacy of individuals by establishing "Fair Information Practices" for the collection, maintenance, use, and dissemination of information by federal agencies. *The Privacy Act*, along with its accompanying case law, is the most significant milestone in the history of the protection of the privacy of personal information held by the federal government. Many subsequent laws, regulations, and guidance build upon the principles first articulated in the *Privacy Act*. (Defined in HHS Information Security Program Privacy Impact Assessment (PIA) Guide).

Privacy Act Information: Any type of IIF/PII collected and maintained on an individual.

Privacy Act System of Records Notice (SORN): All systems with *Privacy Act* information contained within them are required to publish a "Records Notice" in the Federal Register that informs the public what information is contained in the system, how it is issued, how individuals may gain access to information about themselves, and other specific aspects of the system. (Defined in Secure One HHS Information Security Program Privacy Impact Assessment (PIA) Guide).

Privacy Impact Assessment (PIA): A methodology that provides information technology (IT) security professionals with a process for assessing whether appropriate privacy policies, procedures, and business practices—as well as applicable administrative, technical and physical security controls—have been implemented to ensure compliance with federal privacy regulations. (Defined in Secure One HHS Information Security Program Privacy Impact Assessment (PIA) Guide).

Record: Any item, collection, or grouping of information about individuals that is maintained by an agency, including, but not limited to, their education, financial transactions, and/or medical, criminal, or employment history and that contains their name; or it contains the identifying number, symbol, or other identifying information assigned to the individual, such as a finger or voice print or a photograph. (Defined in The Privacy Act of 1974, 5 U.S.C., Section 552a(a)(4), as amended). When the record is under the control of an agency and is contained in an authorized system of records retrieved by personal identifier, it is protected by the provisions of the Privacy Act.

Risk: The net mission impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and (2) the resulting impact if this should occur. IT-related risks arise from legal liability or mission loss due to—

- Unauthorized (malicious or accidental) disclosure, modification, or destruction of information;
- Unintentional errors and omissions;
- IT disruptions due to natural or man-made disasters;
- Failure to exercise due care and diligence in the implementation and operation of the information system. (Defined in NIST SP 800-30, Appendix E).

Risk Assessment: The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses. (Defined in NIST SP 800-30, Appendix E).

Risk Management: The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal approval to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations. (Defined in NIST SP 800-30, Rev A).

Routine Use: Under the Privacy Act, regarding the disclosure of a record, the use of such record for a purpose that is compatible with the purpose for which it was collected.

Security: Measures taken to limit access to information and protect it from attack or theft.

Senior Agency Official for Privacy: An individual selected by the Department to have agency-wide oversight in implementing and ensuring compliance to privacy legislation. (Defined in OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*).

Sensitive Information: Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs or the privacy to which individuals are entitled under [the Privacy Act] but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (Defined in the Computer Security Act of 1987).

Information is considered sensitive if *the loss of confidentiality, integrity, or availability could be expected to have a* ***serious, severe or catastrophic*** *adverse effect on organizational operations, organizational assets, or individuals.* Further, the loss of sensitive information confidentiality, integrity, or availability might: (i) cause a significant or severe degradation in mission capability to an extent and duration that the organization is unable to perform its primary functions; (ii) result in significant or major damage to organizational assets; (iii) result in significant or major financial loss; or (iv) result in significant, severe or catastrophic harm to individuals that may involve loss of life or serious life threatening injuries. (Defined in Federal Information Processing Standard (FIPS) 1999, Standards for Security Categorization of Federal Information and Information Systems, February 2004).

Session Cookie: A small file, stored in temporary memory, containing information about a user that disappears when the user's browser is closed. Unlike a persistent cookie, no file is stored on the user's hard drive.

Substance Abuse Records: Section 543 of the Public Health Service Act, 42 U.S.C. 290dd-2 provides that records of the identity, diagnosis, prognosis or treatment of any patient maintained in connection with a substance abuse education, treatment, prevention, rehabilitation, training or research program are protected and may only be disclosed under limited circumstances, e.g., to medical personnel with a bona fide need, qualified personnel with a research or management need, or if authorized by a court order upon the showing of substantial risk of death or bodily injury. The statute specifically precludes use of the records to initiate or substantiate a criminal charge or to conduct an investigation.

System: An organized assembly of IT resources and procedures integrated and regulated by interaction or interdependence to accomplish a set of specified functions. (Defined in Secure One HHS Information Security Program Privacy Impact Assessment (PIA) Guide).

System of Records (SOR): A group of any records under the control of any agency where information is retrieved by the name of the individual, by some identifying number or symbol, or other identifiers assigned to the individual. The key to this definition is that the records must be "retrieved by", not "retrievable by" an individual's name and/or personal identifier. (Defined in the Secure One HHS Information Assurance and Privacy: Privacy Impact Assessment (PIA) Guide).

Systems of Records Notice (SORN): A publication in the Federal Register of the record system that covers a particular information collection. SORNs can be internal, such as those which cover NIH records. Central agency SOR notices are those that belong to OPM. Government-wide SOR notices are those that belong to the EEOC, FEMA, GSA, DOL, OGE, etc. and which are also referred to as "umbrella" systems of record notices. Note: Before data can be collected, a SORN must be published and maintained in the Federal Register for 40 days.

Technical Controls: The security controls (i.e., safeguards and countermeasures) applied to an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. Technical safeguards include mandatory passwords, encryption, and 30-minute time out protection, as well as firewalls, cryptography, etc. (Defined in NIST SP 800-53, Appendix B).

Threat: An event or activity, deliberate or unintentional, with the potential for causing harm to an information system or activity. (Defined in NIST SP 800-26, Appendix C).

Umbrella System: Agency Privacy Act systems of records that can be used by all or many agencies. Examples include: personnel, finance, time and attendance, pay, badge and I.D., and general correspondence file record systems, etc.

Unauthorized Disclosure: Exposure of information to individuals not authorized to receive it.

Website: A collection of interlinked Web pages (on either Internet or intranet sites) with a related topic, usually under a single domain name, which includes an intended starting file called a "home page." From the home page, access is gained to all the other pages on the website.